May 2022

MRC Weatherall Institute of Molecular Medicine (WIMM)

Information Security Policy and Best Practice

MRC Weatherall Institute of Molecular Medicine, Radcliffe Department of Medicine, University of Oxford
John Radcliffe Hospital, Headington, Oxford OX3 9DS www.imm.ox.ac.uk

Table of Contents

1 Introduction

The aim of this document is to delineate WIMM specific policies and practices in addition to those covered in the overarching Institution and legislative regulations and policies referred to in Annex A.

The policy describes specific WIMM rules and best practice on information security and references the policies of the University of Oxford ("the University").

This Security Policy will be reviewed annually, or more frequently if necessary.

2 Policy Statement

The purpose of the WIMM Information Security Policy is to provide a structured approach to guarding the WIMM's information assets from threats of loss of integrity and confidentiality and to ensure availability. This policy is intended to protect the WIMM's information assets from accidental or deliberate damage either from internal or external sources.

2.1 Scope

This policy is applicable to all WIMM staff, WIMM students and any visitors using WIMM systems, data or other information asset.

For the purposes of this policy the term "staff" means all paid employees, authorised associate members, honorary members and academic visitors to the WIMM.

2.2 Definitions

To avoid ambiguities, particular terminology is used when explaining the policies:

- MUST: This word, or the terms "REQUIRED" or "SHALL", means that the item is mandatory.
- MUST NOT: This phrase, or the phrase "SHALL NOT", means that the item is absolutely prohibited.
- SHOULD: This word, or the adjective "RECOMMENDED", means that there may be valid reasons in particular circumstances not to implement a particular item, but the full implications must be understood and carefully weighed before doing so.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may be valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any action described with this label.

2.3 Roles and Responsibilities

- This policy is authorised by the Director of the WIMM (currently Professor KJ Patel).
- The WIMM IT Committee is the designated owner of the Information Security Policy, the Chair of the Committee is currently Dr Peter McHugh.
- The Information Security Manager for the WIMM is the IT Manager (position currently vacant)
- The University of Oxford Data Protection Officer, see:

https://www1.admin.ox.ac.uk/councilsec/compliance/dataprotection/contacts/

- The Council of the University has ultimate responsibility for information security within the University with particular responsibility to ensure the University complies with all relevant external authorities.

2.4 Information Security Policy Ownership and Responsibility

- The roles and responsibilities of the designated Information Security Manager are to manage information security and to provide advice and guidance on implementation of the Information Security Policy.
- The designated owner of the Information Security Policy (the WIMM IT Committee) has final responsibility for maintaining and reviewing the Information Security Policy.
- It is the responsibility of all line managers to implement the Information Security Policy within their areas of responsibility.
- It is the responsibility of all WIMM staff to adhere to the Information Security Policy.

2.5 Audit and Review

The Information Security Manager is responsible for arranging quarterly audits and reviews of all aspects of the Information Security Policy. Audit results will be recorded and logged.

The Information Security Policy will be reviewed annually by the WIMM IT Committee.

2.6 Regulatory and Legislative Requirements

The Information Security Policy is designed to ensure all regulatory and legislative requirements are adhered to.

3 Authentication and Authorization

All members of the University of Oxford are issued with a University card. The rights and responsibilities of University card ownership are covered by:

http://www.admin.ox.ac.uk/estates/ourservices/fm/card/

The University card entitlements to IT services are delineated at:

http://help.it.ox.ac.uk/iam/registration/service_entitlements

Ownership of a University card provides authorisation for the owner to be a user of the Medical Sciences Division IT Services (MSD IT) computer network and to use the University of Oxford Single Sign On (SSO) authentication system. The WIMM IT team can assist users with accessing these accounts.

The MSD IT computer network is accessed via secure authentication using a Novell username and password processed by the MSD IT administrative team. The WIMM IT team can create and administer Novell user accounts.

Passwords for SSO and Novell accounts must not be shared or disclosed to any third party.

Temporary visitors, e.g. contractors, will not be granted SSO or Novell accounts. Physical access to the WIMM building will only be allowed during office hours and/or when accompanied by a member of WIMM staff.

Desktop systems owned by the department running Microsoft Windows are required to use the Novell network log on wherever possible. Microsoft Windows systems will also be configured to use the WIMM Windows Server Update Services (WSUS) for automatic installation of security updates. This does not apply to non-networked systems or Macintosh or Linux systems.

Both Microsoft Windows and Apple Macintosh systems will be configured to use the WIMM Sophos Enterprise Server for automatic updates to anti-virus software.

Remote access via the University of Oxford virtual private network (VPN) client or Eduroam wireless network is authenticated using a Remote Access account which is only available to owners of active SSO accounts.

4 Internet and Email Usage

4.1 Internet Access

Internet access is provided by the Joint Academic Network (JANET) and administered by University of Oxford IT Services. The MSD IT network infrastructure connects the WIMM to the University network.

All users of the network are required to adhere to the rules governing the acceptable use of the JANET network, a link to which is given in Annex A. New staff will be informed of these rules as part of the induction process.

All users of the University network are required to adhere to the University of Oxford Rules on IT Use, a link to which is given in Annex A. New staff will be informed of these rules as part of the induction process.

All WIMM members are required to adhere to the MSD IT Security Policy, a link to which is given in Annex A. New staff will be informed of these rules as part of the induction process.

All new staff in the WIMM will be required to attend an IT Induction presentation which will include material relating to good information security practices.

Information security awareness training is **compulsory** for all University staff, WIMM staff are required to complete the University of Oxford online information security awareness module:

https://www.infosec.ox.ac.uk/guidance-policy/training-and-awareness

4.2 Email

Access to the University of Oxford email services is controlled and administered by IT Services. Regulations governing the use of email are covered by the University ICTC regulations (2002) with subsequent amendments, a link to which is provided in Annex A.

Breaches of regulations will, in the first instance, be reported to the line manager and a record of the breach passed to the WIMM IT team.

Where users redirect or forward email from their University account to external mail servers it is incumbent on them to ensure a comparable level of security to that provided by the University service.

The WIMM IT Induction presentation provides users with advice relating to phishing exploits and other email exploits.

Where a phishing email is intended to expose a user's SSO credentials they are encouraged to report this to IT Services in order to protect other users of the University email system.

http://help.it.ox.ac.uk/email/phishing/index

5 Building Security

All staff are issued with an Oxford University Hospitals (OUH) Trust photo ID card. Staff are responsible for their ID badges and must notify WIMM reception in the event of loss. Staff must not share keys and swipe cards with any third parties. ID cards must be carried at all times, preferably worn prominently to facilitate identification of authorised personnel.

All external doors to the WIMM will be security locked at all times. Internal offices must be locked independently when not in use. Offices involved in processing sensitive data will be subject to greater security measures.

Access to the building is via swipe cards managed from a C-Cure database allowing access to only those areas of the WIMM appropriate to a member's work. WIMM staff must ensure they do not allow anyone tailgating them into the building. All access for visitors is via reception where visitors are required to sign in and out of the building.

WIMM reception must be notified at once in the event a card key is lost or stolen.

The WIMM IT Office lock can only be opened by WIMM IT Staff and the WIMM Building Manager. The WIMM server room is only accessible to WIMM IT staff, Computational Biological Research Groups' (CBRG) system administrator staff and the WIMM Building Manager. Access to the WIMM server room for all other staff requires that they are accompanied by a member of the WIMM IT Team.

It is the responsibility of the WIMM IT Manager to ensure that a biannual specialist clean of the WIMM server room is carried out.

6 Networks and Systems IT Security

The WIMM computer network is part of the University of Oxford network & is managed by MSD IT system administrators on behalf of the University Medical Sciences Division.

The MSD IT service description is given here:

http://www.imsu.ox.ac.uk/content/msd-it-service-specification

Departmental responsibilities in relation to these services are outlined at:

http://www.imsu.ox.ac.uk/content/expectations-and-responsibilities-departments

All personally-owned devices connecting to the WIMM wired LAN must be authorised by WIMM IT staff via entry of the device's hardware address in the MSD IT DHCP (Dynamic Host Configuration Protocol) tables. It is a mandatory requirement that all computers attaching to the WIMM wired LAN have up-to-date anti-virus software installed.

Access to the OWL wireless network requires authentication to the University of Oxford Virtual Private Network (VPN) using the user's Remote Access account credentials. Authentication to Eduroam also requires the user's Remote Access account credentials. OWL and VPN allows the

user to access the University of Oxford network resources, Eduroam does not – it merely allows internet access. The WIMM IT Team can assist users to set up access to the wireless networks.

Sharing of credentials, IP addresses or LAN adaptor devices is **not** permitted. Any loss of devices registered on the MSD IT DHCP tables should be reported to WIMM IT staff and the device will be removed from the tables and denied access to the WIMM wired network.

Devices such as Apple Time Capsules or wireless routers are **not permitted** access to the WIMM network as they cause disruption to the network via the creation of *ad hoc* wireless networks.

All requests for changes to the WIMM firewall necessary for incoming access for file servers is at the discretion of the MSD IT systems team.

6.1 Computers, Software and Hardware

MSD IT Security Policy (see Annex A) defines control measures for WIMM hardware and software.

The WIMM IT team are responsible for ensuring that computer systems are risk assessed, audited and configured in line with the security policies outlined in this document.

It is the responsibility of WIMM line managers to ensure that their staff adhere to the policies outlined in this document and those of the overarching authorities. Breaches should be reported in the first instance to the WIMM IT team.

All software installed on WIMM systems will normally be required to comply with the MSD IT Security Policy and those regulations pertaining to the use of software in the overarching authority's policies (see Annex A).

WIMM IT managed Microsoft Windows computers allow only standard access rights to users when the Novell Zenworks dynamic user creation is configured. Elevation of the user account to administrator status is enabled at the discretion of the WIMM IT Team. Administrative access to a computer on the WIMM network comes with responsibilities which the user must be made aware of. This does not generally apply to Apple Macintosh and Linux systems.

Personally-owned systems configured for the WIMM computer network will necessarily allow full administrator access rights for the owner of the system.

All systems configured for use on the WIMM computer network, whether departmentally or personally-owned will be required to have an administrative account created that only the WIMM IT team know the credentials for. Thereby allowing the team access to the system in event of a security breach in the absence of the system owner.

All systems configured for use on the WIMM computer network, whether departmentally or personally-owned will be required to have up-to-date legitimate anti-virus software installed.

No access to the WIMM computer network will be permitted for personally owned computers on which illegal software and other non-compliant software has been installed.

Where essential systems use non-compliant software (e.g. PCR instruments running Windows XP) access to the WIMM network will be restricted to the MSD IT XP Virtual Local Area Network (VLAN) allowing only Sophos anti-virus updates to occur and access to the MSD IT Novell home folders.

Purchasers of hardware and software are advised to consult with the WIMM IT team prior to making any purchase. In particular, purchasers need to be aware that WIMM high capacity storage is limited and they may need to include storage in their purchase.

Departmentally owned computer systems that are to be decommissioned must be given to the WIMM IT team for secure decommissioning. The hard disks will be removed from the systems and mechanical destruction of the disks will be done on-site. It is the responsibility of the WIMM IT Manager to arrange for this service.

6.2 Back-up and Archiving

It is the responsibility each individual member of WIMM staff to ensure their data is appropriately backed up.

Where appropriate departmentally-owned systems will have the University IBM Spectrum Protect (formerly HFS) client installed.

For personally-owned systems users are recommended to use both the University HFS service and, where possible, a proprietary alternative such as File History (Windows PCs) and Apple Time Machine. The WIMM IT team will provide back-up advise to users and is included in the WIMM IT presentation. Where feasible backups should be stored in more than one location.

The University HFS service provides long term archiving of rarely accessed data, details of which can be found at:

http://help.it.ox.ac.uk/hfs/archive

When data is no longer active it must be archived. The security level of archive storage must be subject to risk assessment which takes into account the nature of the data to be stored.

Files stored on the MSD IT Novell system are backed up overnight. See MSD IT Security Policy (Annex A) for their back-up policy.

Hardcopy data must be recorded and stored securely.

6.3 Encryption

All data subject to the Data Protection Act 1998 (see Annex A) and of a sensitive, confidential or personal nature must be stored and transmitted in a secure manner. Users must not attach unencrypted documents to emails, documents must be encrypted if being sent via email.

The University OxFile system allows secure electronic transmission of data. MSD IT have a system, FILR, which is equivalent to OxFile. The University SharePoint service provides a secure platform for collaboration. MSD IT provide a High Compliance service equivalent to the University SharePoint service. The WIMM IT team can advise on these services.

Systems storing data falling into the sensitive data category must securely encrypt the data storage location and ensure secure transmission of the data.

There are a number of mechanisms for encryption available from encrypting a single document or folder (VeraCrypt) to encrypting an entire hard disk (BitLocker, FileVault and the University Whole Disk Encryption service (WDE). The WIMM IT team can provide guidance on the appropriate encryption tools and emphasis the requirement for a good backup strategy when encryption is used.

When moving sensitive data when not using OxFile, FILR or Dropbox a physically encrypted USB storage devices must be used. These can be purchased from MSD IT:

http://www.imsu.ox.ac.uk/content/encryption-services

It is mandatory that systems being used outside the WIMM and storing work-related data have this data encrypted. The WIMM IT can provide guidance on this.

7 Remote Access and Home Working

When working from home and abroad the University of Oxford VPN must be used to ensure a secure connection. When travelling abroad ensure that local legislation regarding encrypted data are observed. When in doubt check with the WIMM IT Team.

All copies of files of a sensitive nature stored in local copies whilst working remotely must either be deleted or stored in an encrypted location on home systems.

University policies covering working from home are set out on the University Personnel

website: http://www.admin.ox.ac.uk/personnel/during/flexible/homeworking/

Access to MSD IT networked storage is via the NetStorage system, for details see:

http://www.imsu.ox.ac.uk/content/vpn-services-and-access-network-storage

MSD IT also provide a file synchronization "cloud" service called FILR, details of which are available at:

http://www.imsu.ox.ac.uk/content/filr

Access to NetStorage and FILR should be via the Oxford VPN.

Using the Oxford VPN client will allow users to log into their MSD IT home folders with full access using the Micro Focus client. Users working on sensitive data must take precautions to ensure data stored locally are either deleted or saved in encrypted locations on home systems.

Where users wish to access office systems remotely they must contact WIMM IT staff in the first place and access to systems will be provided at the discretion of MSD IT.

Home working which involves taking a computer or data drive out of the WIMM will require that sensitive data is encrypted and that steps are taken to mitigate against risk of loss or damage. University hardware and software is covered by the University Insurance and is subject to a £2000 excess.

Access to the University email system outside the WIMM should be via the Outlook Web Access (OWA) browser interface in order to avoid local caching of emails unless the system is encrypted.

Encrypted USB drives should be used for moving files from one location to another when not using OxFile, FILR or Dropbox.

8 Mobile Devices

All access to University email and sensitive data from mobile devices (tablets, smart phones etc.) should follow the guidelines laid out in

https://www.infosec.ox.ac.uk/guidance-policy/it-security

The InfoSec website outlines the minimum steps needed to secure a mobile device:

https://www.infosec.ox.ac.uk/want/mobile

Apart from using these devices to access University email (this will entail these devices retaining a locally cached copy of the mail) they should not be used to transport sensitive or confidential data. Email clients on mobile devices should not be configured to use POP or IMAP to access University email accounts.

Where possible devices should be configured to allow a remote wipe of a device in the event it is lost or stolen. If a mobile device configured for access to University systems is lost or stolen the WIMM IT Team must be notified. The team can assist with remote deletion of devices. Should a mobile device be lost or stolen it is essential that the user change SSO password and passwords for any other services accessed from the device.

9 Internet and Cloud Services

Users should be aware that internet services provided by third parties may not be in the EU and may be subject to laws and regulations of other legal jurisdictions and not secure. The Data Protection Act 1998 prohibits the storing of data (subject to the regulations of the Act) outside the EU. Examples of these services are Gmail, Yahoo Mail, Hotmail, Dropbox, Google Drive, Office 365 etc.

These services are targets for security attacks and data and information stored by these service providers may be sold or manipulated by hackers.

The University provides many of these services itself that comply with the University's policies and regulations pertaining to information security. These services should be used in preference to those of third parties. The Nexus service provides members of the University with a secure email server, the University Sharepoint service provides an arena for document sharing and collaboration as does the Weblearn service. Cloud services are provided by NSMS a department within IT Services:

https://www.it.ox.ac.uk/nsms/private-cloud

10 Information Handling

All staff are bound to the University confidentiality agreement by their employment contract. They receive a copy of their contract when they commence work. Staff are expected to comply with their contractual obligations.

Visitors to the WIMM are bound by the Visiting Worker Agreement (November 2016) which contains clauses binding visitors to the same confidentiality agreements as staff. The Visitors Agreement cites the University Information Security Policy and the ICTC regulations 1 of 2002. Visitors are expected to adhere to the policies and regulations with regard to Information handling outlined in this document.

Information security and confidentiality applies both to electronic and hard copy of data files. Staff and visitors are expected to act in accordance with the regulations and policies outlined in this document (Annex A) when processing and handling paper documents, computer files, electronic records, CDs, DVDs, disk drives, USB drives or any other storage or processing agreements.

Shredders are provided by WIMM Administration to securely destroy hard copy of data files. WIMM IT decommission systems and remove data storage media which is then physically destroyed. Any media storing sensitive data (CDs, DVDs, USB flash drives, computer systems) must be returned to the WIMM IT Office for secure destruction of the media.

All staff dealing with personnel data are required to undertake training in relation to the Data Protection Act 1998.

Computer screens must be locked with a password when left unattended.

Any confidential or sensitive data can only be transferred using encrypted media, e.g. encrypted USB drive, the University encryption FAQ describes the different options available:

http://www.imsu.ox.ac.uk/content/encryption-faq

Any computer taken out of the WIMM and storing confidential data must ensure the data is stored encrypted on the system.

11 Disaster Recovery, Risk Assessment and Business Continuity

The WIMM has a disaster recovery plan and a risk register. Business continuity planning forms part of that plan. The plan will be reviewed annually.

All projects handling sensitive data will have to have completed and recorded a risk assessment.

The WIMM management committee must be notified of any significant risks identified in a risk assessment and plans should be put in place for appropriate mitigation.

MSD IT are responsible for data backup and recovery of the network storage they provide to WIMM staff.

WIMM staff are encouraged to store all work-related data on this networked storage.

IT Services provide the Hierarchical File Service (HFS) for backup on a weekly basis. This service also provides a long-term storage archive. A description of the HFS service can be found at:

http://help.it.ox.ac.uk/hfs/index

The WIMM IT induction presentation also encourages WIMM members to have an additional backup of their data on an external hard disk and use the built-in Macintosh backup software, Time Machine, or the Microsoft Windows software, File History.

12 Sanctions

Suspected breaches of any part of the Information Security Policy and related policies should in the first instance be reported to the line manager of the staff member concerned.

All breaches and incidents should also be reported to the WIMM IT Manager. Incidents that are deemed to be serious will then be reported to the WIMM management committee. A log of breaches will be kept by WIMM IT. Thefts must be reported to the police and a crime number recorded. Loss of sensitive data must be reported to the University's Data Protection team (data.protection@admin.ox.ac.uk) and the Information Security team (infosec@it.ox.ac.uk).

Any member of staff who is deemed to have deliberately or maliciously breached the WIMM Information Security Policy will be subject to the appropriate HR policy.

Annex A

This section contains a list of supervening laws and policies that may apply to use of IT facilities. Note that this list may not be exhaustive and will be subject to amendments and any superseding legislation that may be enacted. The legislation can be viewed via www.legislation.gov.uk. Those who use the facilities from outside the UK may be bound by the laws of the UK and/or any other applicable local laws.

Obscene Publications Act 1959 & 1964
Protection of Children Act 1978
Police and Criminal Evidence Act 1984

Copyright, Designs & Patents Act 1988
Computer Misuse Act 1990
Human Rights Act 1998
Data Protection Act 1998
Regulation of Investigatory Powers Act 2000
Freedom of Information Act 2000
Counter Terrorism and Security Act 2015
Terrorism Act 2006
Police and Justice Act 2006
Digital Economy Act 2010
Equality Act 2010
Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011

Users of ICT within the University must also comply with the following:

- The University ICTC regulations (2002) with subsequent amendments and available for review at:

  http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml

- University of Oxford Rules on IT Use:

  http://www.it.ox.ac.uk/rules

- The JANET Acceptable Use Policy:

  https://community.jisc.ac.uk/library/acceptable-use-policy

- Medical Research Council Security Policy

  https://www.mrc.ac.uk/documents/pdf/mrc-security-policy/

- University of Oxford Information Security Policy as outlined at:

  https://infosec.ox.ac.uk/sites/default/files/Information Security Policy.pdf

- Medical Sciences Division IT Security Policy:

  http://www.imsu.ox.ac.uk/sites/default/files/content/files/MSD_IT_Security_Policy.pdf